Detection of Wormhole Attacks in Wireless Sensor Networks

Mohan Seth

Department of Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela-769 008, Odisha, India

Detection of WormHole Attacks in Wireless Sensor Networks

Thesis submitted in

May 2013

to the department of

Computer Science and Engineering

of

National Institute of Technology Rourkela

in partial fulfillment of the requirements

for the degree of

Bachelor of Technology

in

Computer Science and Engineering

by

Mohan Seth

[Roll: 109CS0188]

with the supervision of

Prof. Manmath Narayan Sahoo

Department of Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela-769 008, Odisha, India

Department of Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela-769 008, Odisha, India.

May 11, 2013

Certificate

This is to certify that the thesis entitled, ***DETECTION OF WORMHOLE ATTACK IN WIRELESS SENSOR NETWORK*** submitted by ***MOHAN SETH(109CS0188)*** in partial fulfillment of the requirements for the completion of Bachelor of Technology Degree in Computer Science and Engineering at the National Institute of Technology, Rourkela is an authentic work carried out by them under my supervision and guidance .To the best of my knowledge, Neither this thesis or any part or it has been submitted for any degree or diploma award elsewhere.

Prof.Manmath Narayan Sahoo
Assistant Professor
Department of Computer Science and Engineering
NIT Rourkela

Acknowledgment

With great satisfaction and pride I present my thesis on the project under the Research Project paper during Final Year, for partial fulfillment of my Bachelor of Technology degree in Computer Science and Engineering at NIT Rourkela.

I am thankful to Prof. Manmath Narayan Sahoo for being the best guide and advisor for this research work in every field I have taken to complete my requirement. His ideas and inspirations have helped me make this nascent idea of mine into a fully-fledged project. Without presence of him I may never had tasted the flavor in a research work.

Again I am thankful to my batch-mates to support me in my implementation part sometime. I am also grateful to all the professors of my department for being a constant source of inspiration and motivation during the course of the project.

I would like to dedicate this project to my parents, who always stood by me in each and every point of my life.

So I am thankful again to all who are being a part of my Final year research project.

Mohan Seth

Abstract

Wormhole attacks can destabilize or disable wireless sensor networks. In a typical wormhole attack, the attacker receives packets at one point in the network, forwards them through a wired or wireless link with less latency than the network links, and relays them to another point in the network. This paper describes a wormhole detection algorithm for wireless sensor networks, which detects wormholes based on the distortions they create in a network. The two characteristics are to keep tracks of all its neighboring nodes and checks if a node received is from its neighbor or not. The main advantage of the algorithm is that it can provide the approximate location of wormholes, which is useful in implementing countermeasures.

Contents

List of Figures

–

Chapter 1

Introduction

1.1 Introduction to Wireless Sensor Network

Wireless sensor networks (WSNs) are developing technology paradigm consisting of small, low-power devices that consist of limited computation, sensing and radio communication capabilities. The technology has the ability to provide flexible infrastructures for numerous applications, industry automation, including healthcare, surveillance and defense. Currently, most WSN applications are designed to operate in trusted environments. However, security[10] issues are a major concern when WSNs are deployed in untrusted environments. An attacker may disable a WSN by interfering with intra-network packet transmission via wormhole attacks, Sybil attacks, jamming or packet injection attacks.

1.2 Structure of a WSN

The physical process is the application which run on every node of the network . there is no central node or base station to control the communication every node communicate to each other by using the wireless channel.

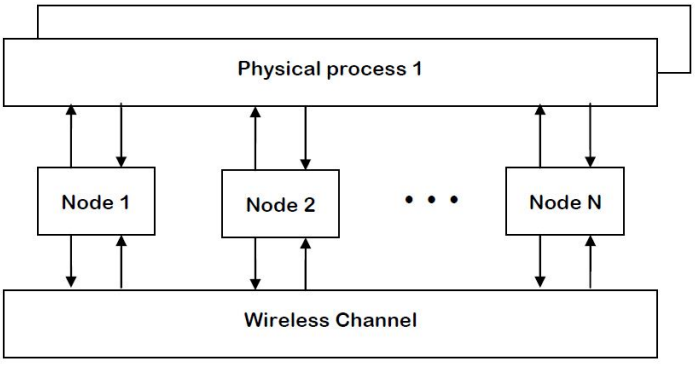


FIGURE 1.1: structure of WSN

1.3 Threats in Wireless Sensor Network

A wireless Sensor Network (WSN) has many constraints as compared to a conventional computer networks

1.3.1 Nature of Communication

As the mode of communication is open it attract many threat to its transmission security

1.3.2 Ad-Hoc Deployment

Due to high mobility[11] of the nodes it is not practical to maintain any kind of topology. Security measures should be well equipped to maintain this kind of change in the network.

1.3.3 Resource Limitation

Resources like memory, bandwidth, and energy to power the sensor are limited in the tiny wireless node which can be very much of a problem to any resource hungry network

1.3.4 High Risk of Physical Attack

As the node is unattended hence prone to physical attack. an adversary can easily eaves drop the transmission or launch serious attacks.

1.4 Introduction to Wormhole Attack

In a network and attacker connects two points situated at different part of the network using a direct low latency communication link called as the wormhole link, it is established by Ethernet link, optical link, long range wireless transmission. Once the link is established the adversary captures wireless transmission (transmitting packets) at one end, and transmits through the wormhole link and retransmit them at the other end.

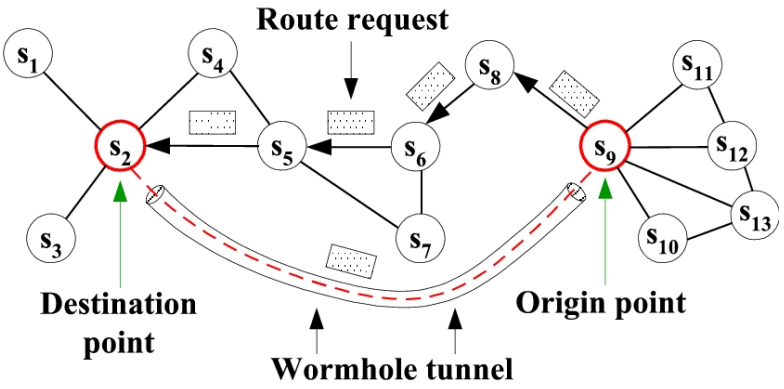


FIGURE 1.2: Wormhole with end x and y

1.5 Why Wormhole Attack is so Vulnerable ?

The vulnerability of wormhole attack is high because it is a passive attack as it does not require the information about the cryptographic infrastructure of the network ,hence it puts an attacker in a beneficial or strong position.

Chapter 2

Literature Review

2.1 Existing Approaches

2.1.1 Approach Packet Leashes

Leash is any information added to a packet designed to restrict the packets maximum allowed transmission distance.
Geographical leash[3] insures that the recipient of the packet is within a certain distance from the sender.
Temporal leash ensures that the packet has an upper bound of its lifetime (restricts the maximum travel distance).

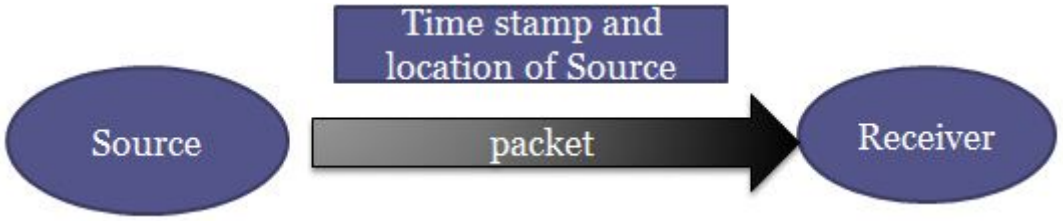


FIGURE 2.1: Packet Leashes

2.1.2 Assumptions

- Pre-known location of each node
- Synchronized clock for set of sender and receiver.

2.1.3 Detection

Wormhole is detected by detecting the mismatch between the time stamp differences calculated and location difference absorbed.

2.2 Approach by Hu-Evans with directional antenna

It uses directional antenna because it only transmits in a defined direction not in 360 degree.

- Hence it is easy to detect any malice in the network if every node is equipped with a directional antenna.
- Authenticating along a given direction along with localization can be beneficial.

2.3 Approach By Lazos and poovendran- SerLoc

InSeRLoc[9], there are about 400 anchor Nodes deployed in a 5000-node network. Only anchor nodes are equipped with directional antenna. Other nodes uses this anchor nodes to locate themselves This method requires[8] these nodes to be manually set up in advance. When attack is done it is detected by directional antenna . When the anchor node is close to the end of wormhole then it is compromised[18] .

2.4 Approach called MDS-VOW

It works in a different way, it finds the distortion in the computed maps. It works only in a centralized scheme[5], hence it needs to have a central computer, to complete its computation. One of the main disadvantages of this technique is wormhole cannot be detected in

2.5 WGDD

This algorithm[1] is based on detecting network disorder caused by the existence of a wormhole .The presence of wormhole in the network increases the range of transmission of the packet because the packet is transmitted through the wormhole link to the farthest part of the network so the receiver assumes the node at far distance to be as one of its neighbor node, which creates problem during application of routing algorithm . The algorithm is divided into three parts:

- Probe procedure
- Local map computation procedure.

- Detection Procedure

2.5.1 Probe procedure

As we know wormhole attack are passive attacks as it absorbs the packet traveling near to its end. The procedure uses a bootstrap node to flood the network within the network. Then each node calculates the hop distance from itself to the bootstrap node
Bootstrap node:It floods the whole network with probe message consisting (i=idx) .
The bootstrap node has the hop coordinate as hopx =0 and offsetx=0.
General nodes: Let a be a node the it calculate its hop distance. And b be its neighbor and to reach b it needs hopb distance then hopa= hopb + 1.

2.5.2 Local map Computation Procedure

In this procedure each node calculates a local map from hop coordinates which are calculated in the probe procedure .After the hop coordinates are created every node requests its neighbor which are within one/k hop distance to send their hop coordinate . After the node receives hop coordinates from its neighbor then it calculates the shortest distance between any pair of node between one/k hop distance.This step has a computational cost of O([Na]3 n) and a memory cost of O([Na]2) per node. No communication cost is associated with this step.

2.5.3 Detection Procedure

The detection procedure uses the local map computed in the earlier stage to detect wormhole in the network.

As the wireless sensor nodes poses very less resources hence it uses local information as it cannot store the global data . As mentioned due to presence of wormhole two part of the network gets shortcut and hence a transmitting node can reach farther then its transmitting range. This detection algorithm uses diameter[1] in the local map computed as a parameter to detect wormhole. It defines diameter d of anode as-

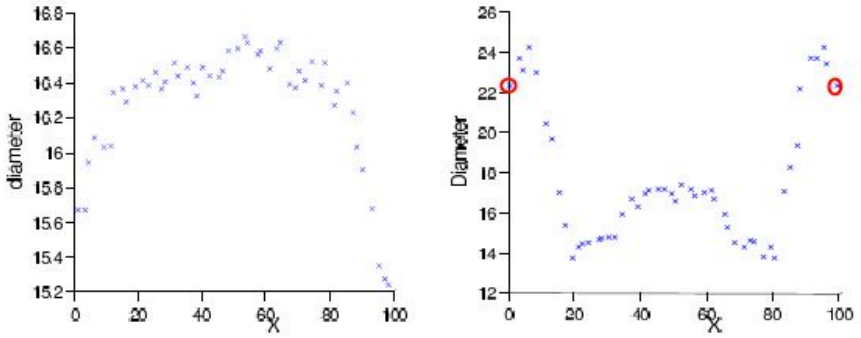
d =max(distance(b,c))/2

and distance is calculated , if coordinates of b and c are (x,y)and (x,y) then the distance will be

D=((x-x)2+(y-y)2).

The feature of the algorithm explore the property of the WSN node that it can only transmit in the range as defined and the input power given. Hence a node should not transmit beyond that range and if any node is transmitting beyond that range we may say that there is possibility of presence of worm hole in the network.

The figure in the next page depicts how the change in the diameter of the nodes are observed if the end of the wormholes are placed at the network end.



(a) Network without a wormhole. (b) Network with a wormhole.

FIGURE 2.2: variation of diameter due to the presence of wormhole

The above picture depicts the variation of diameter near end of the network . The highest value of diameter in the computed map is (25m) ,it decreases at the end of the network but remains above 22mtr.This shows how presence of wormhole in the network can affect the transmission range and affect the routing algorithm. The above algorithm can be used to find wormhole in irregular shape network also

Chapter 3

Motivation

Detecting wormhole with least resource available should be the main objective in any wormhole detection algorithm. As the wireless sensor nodes are provided with less resource and if that small resource is used in detecting attacks in the network or any network anomaly then the node cannot meet the requirement for its proper functioning .The detection algorithm should be less resource hungry and simple so that it will not require more computational power or memory power.

3.1 Issues in the existing algorithm

The existing algorithm are more resource hungry. In WGDD algorithm the local map computation was rather not so important, its only using the nodes limited resources. Calculating shortest distance between any two pair of node in the network was also not needed as after all the requirement was the node should not transmit out of its range ,as the detection algorithm is using the diameter parameter computed in the local map computation procedure this diameter can also be calculated from the power input given to a node, as the range of transmission of a node is directly proportional to the transmission range and any anomaly found in the transmission range will give information about presence of wormhole in the network.

Chapter 4

Proposed Mechanism

The main concept in detecting presence of wormhole in a network is to find out if node is transmitted out of its transmitting range. That can be found out if the packet received is not one of its neighbors. This mechanism proposes that every node will maintain a neighborhood table. A neighborhood table consists of node ID that comes inside the transmission range of the transmitting node.
Two main important characteristic of the proposed work :
Neighborhood table:
Every node in the network will maintain a neighborhood table which will consists of node ID of the neighbor nodes .As the network we are implementing is an uniform one hence the node will be in set in matrix format hence we can easily get the neighborhood table.
Detection procedure:
The algorithm detects wormhole in the network when it receives a packet that doesnt belong to any node in its neighborhood. Any node in the network called bootstrap node triggers the algorithm and then it sends packet with node information if there is no wormhole present near its transmission range then the transmission takes place in normal way and the node receives the packet check whether it has come from its neighbor if it has it accepts the packet and retransmit a packet with self-address otherwise if it receives from out of neighborhood it detects a wormhole in the network.

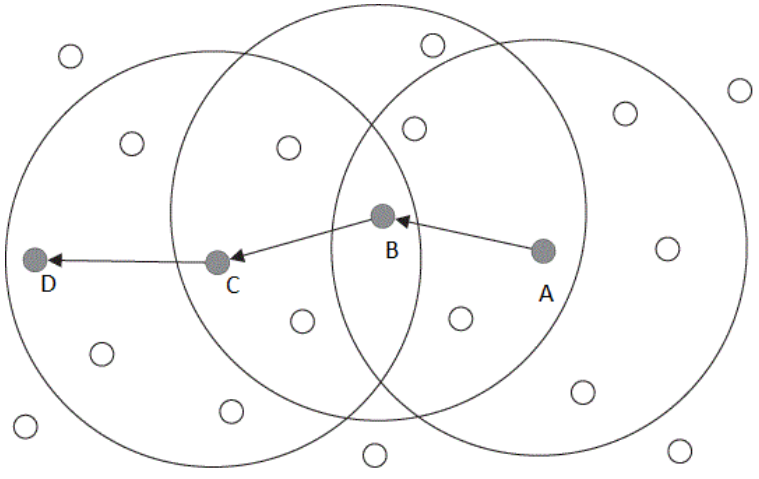


FIGURE 4.1: Showing Normal packet transmission

The above picture shows how a packet in normal condition transmits from source to destination, the packet will not travel out of its transmission range. If a packet

from A is received by C or D directly then there is a possibility of presence of wormhole in the network.

4.1 Nomenclature used in the algorithm

N: total number of sensor node
A,b : random node
Na : set of node in the neighborhood table of a
Px : packet received from node x
hopa : no. of node to reach node a from bootstrap node.

4.2 Proposed Algorithm

Data: b, P and b $\in N_a, N_a$ is the set of neighbor nodes, p is a packet
Result: A node belongs to neighborhood or not
while *rounds* $\leq n$ **do**
  if *node has not received any packet* **then**
    if $p \in N_a$ **then**
      $p_a = p_x$
      Retransmitt
    else
      Detect Wormhole
    end
  else
    Ignore packet p_x
  end
end

Chapter 5

Simulations and Results

5.1 Simulation

I have used castalia for simulation, Castalia uses Omnet++ as its base but as Castalia has been used in a very basic way Omnet++ is not used for the simulation. The three basic module of Castalia are Sensor manager, Application module and communication Composite module.

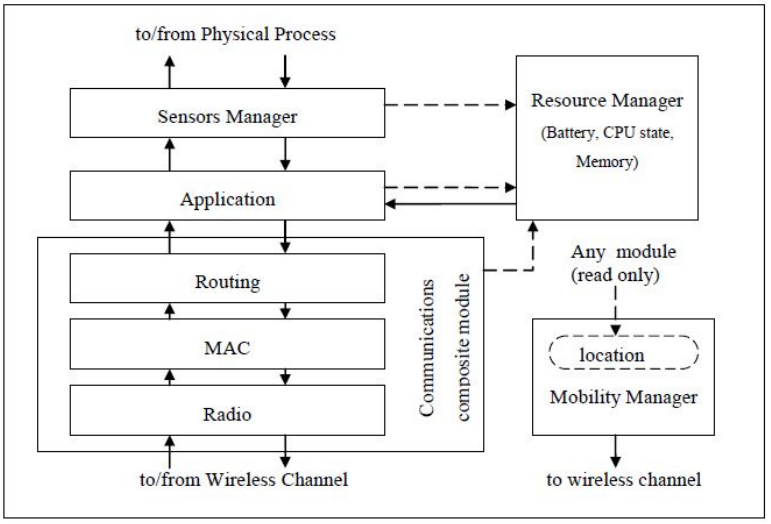


FIGURE 5.1: Showing Normal packet transmission

The network specification are ,total number of 25 nodes are used in a uniformly distributed network in a two dimensional 5x5 distribution in a 60x60 meter network dimension.

The below picture gives information about the run time status of each module used

Module	Output	Dimensions
Application	Packets received	25x25
Communication.Radio	RX pkt breakdown	25x1(3)
	TXed pkts	25x1
ResourceManager	Consumed Energy	25x1
	Estimated network lifetime (days)	1x1
	Remaining Energy	25x1
Simulation	Execution ratio (simtime/realtime)	1x1
	Execution time, seconds	1x1

FIGURE 5.2: Showing Normal packet transmission

Simulating the network in Castalia we retrieve the neighborhood table , we create the neighborhood table from packet received table. It shows which node has received how many packet that are transmitted from a node,as a node receives packets from any transmitting node we make that node to be the neighbor node

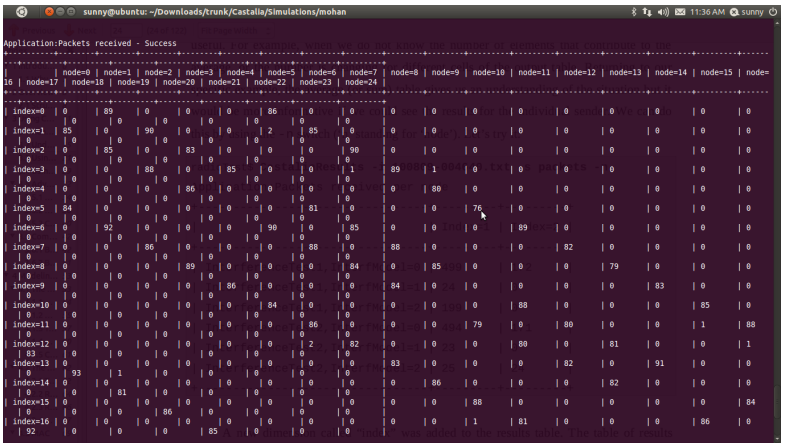


FIGURE 5.3: Neighborhood Table

of that transmitting table.
The neighbor table gives information about which node are present in any nodes neighbor table ,if we look at node 0 column then we will find that the packets transmitted from this node are only received by node 1 and node 5 which receives 85 and 84 packets respectively and no other node receive any packet transmitted by node 0 .hence node 1 and node 5 are neighbor of node 0.

The table is implemented in C to find out wormhole ,by implementing the table as a structure consisting the node id and neighborhood matrix. And if the node receives any packet from out of neighborhood then it detects presence of wormhole in the network.

5.2 Analysis

The wormhole is implemented in c hence it does not give a clear picture of the simulation but the implementation of algorithm will be in nodes hence the algorithm if run in any node will detect wormhole because the detection is using packet information to detect wormhole in the network .

Chapter 6

Conclusions and Future Works

6.1 Conclusions

The simulation is carried out taking 25 nodes in two dimensional 5X5 matrix ,and the neighborhood table was found which is implemented in c to detect any presence of wormhole in the network. The power input to node is taken as -5dbm and accordingly the neighbor table was found. The algorithm is found to be less resource hungry as the algorithm is only using a simple search method to find the transmitting node in its neighbor table .

6.2 Future Works

The implementation of this algorithm with full hardware and software specification will give a very much real world scenario. The algorithm might not work upto its potential if we increase the network by adding nodes which may cause change in the neighborhood table. I also intend to carry out the simulation in a wireless sensor network with more number of nodes and with change in network dimensions.

Chapter 7

Bibliography

Bibliography

[1] Yurong Xu, Guanling Chen, James Ford and Fillia Makedon," Detecting Wormhole Attacks In Wireless Sensor Networks".

[2] Balambika Vinod "Responding To An Attack IN Sensor Networks" Master of Science in Computer ScienceOklahoma State UniversityStillwater, Oklahoma 2012.

[3] Priya Maidamwa and Nekita Chavhan survey on security issues to detect wormhole attack in wireless sensor network,International journal on AdHoc Networking System,vol-2,no-4,Oct2012.

[4] T. Sakthivel,Research Scholar Detection and Prevention of Wormhole Attacks inMANETs using Path Tracing Approach, Manonmaniam Sundaranar University

[5] Kia Xiang, Shyaam Sundhar Rajamadam,Srinivasan, Manny Rivera,Jiang Li, Xiuz hen Cheng, Attacks and Countermeasures in Sensor Networks: A Survey, pp 1-28, Springer, 2005.

[6] G. Padmavathi, Mrs. D. Shanmugapriya, A Survey of Attacks, Security Mechanisms and Challengesin Wireless Sensor Networks, International Journal of Computer Science and Information Security Vol. 4, No. 1 and 2, 2009.

[7] Nityananda Sarma , Sangram Panigrahi, Prabhudutta Mohanty and Siddhartha Sankar Satapathy, Security Issues in Wireless Sensor Network Data Gathering Protocols: A Survey, Journal of Theoretical and Applied Information Technology, 2005.

[8] Abhishek Jain,Kamal Kant, Security Solutions for Wireless Sensor Networks, IEEE Second International Conference on Advanced Computing and Communication Technologies, pp 430-433,2012.

[9] Shahriar Mohammadi and Hossein Jadidoleslamy, A Comparison Of Link Layer Attacks On Wireless Sensor Networks, International journal on applications of graph theory in wireless ad hoc networks and sensor networks(GRAPH-HOC) Vol.3, No.1, March 2011.

[10] Sushma, Deepak Nandal, Vikas Nandal, Security Threats in Wireless Sensor Networks, IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 01, May 2011.

[11] Syed Ashiqur Rahman ,Md. Safiqul Islam, Anomaly Intrusion Detection System in Wireless Sensor Networks: Security Threats and Existing Approaches, International Journal of Advanced Science and Technology Vol. 36, November, 2011.

[12] Ali Modirkhazeni, Norafida Ithnin, Mohammadjavad Abbasi, Secure Hierarchal Routing Protocols in Wireless Sensor Networks: Security Survey Analysis, IJCCN International Journal of Computer Communications and Networks, Volume 2, Issue 1, February 2012.

[13] Dhara Buch, Devesh Jinwala, Detection of Wormhole Attacks in Wireless Sensor Networks, IEEE Conference on Advances in Recent Technologies in Communication and Computing, pp 7-14, 2011.

[14] Khin Sandar Win, Analysis of Detecting Wormhole Attack in Wireless Networks, World Academy of Science, Engineering and Technology 24, 2008.

[15] Majid Meghdadi, Suat Ozdemir and Inan Guler , A Survey of Wormhole based Attacks and their Countermeasures in Wireless Sensor Networks, IETE TECHNICAL REVIEW, VOL 28, ISSUE 2, Mar-Apr 2011.

[16] Mani Arora, Rama Krishna Challa, Performance Evaluation of Routing Protocols Based on Wormhole Attack in Wireless Mesh Networks, Second International Conference on Computer and Network Technology, pp 102-104, 2010.

[17] Rama Krishna Challa ,Mani Arora, Divya Bansal, Performance Evaluation of Routing Protocols Based on Wormhole Attack in Wireless Mesh Networks, IEEE Second International Conference on Computer and Network Technology, pp 102-104, 2010.

[18] Dhara Buch, Devesh Jinwala, Prevention of wormhole attack in Wireless sensor network,International Journal of Network Security and Its Applications (IJNSA), pp 85-98, Vol.3, No.5, Sep 2011.